Planning and Implementing Enterprise Identity Management: 
Why we did it, what we did, and how we did it

Neil Thelander, Director, Information Technology Services
Division of Technology, Information and Learning Support

18th August 2008

“I think you should be more explicit here in step two.”
IT for Access, Domains, Support

Access

Client Agents (Tools, Applications, Portlets, Web Services)

Domain Enabler

Teaching and Learning Services
Research Services
Administration Services

Infrastructure Services

Data and Compute Services
Identity and Security
Messaging and Collaboration

Source JISC

QUT Strategy hence IT

Blueprint
L&T
Research
People/Culture
Finance/Infrastructure

Business process management

Policy/processes - MOPP

Enterprise strategy

Business strategy

Technology strategy

IT strategy

Business architecture

IT architecture

Architecture governance

Business operating environment and IT infrastructure

Change programs

Business, Information, Application, Technology

Business Architecture

Information Architecture

Application Architecture

Technical Architecture

Teaching and learning

Research

Administration

Business directions, governance, stakeholders, organisational structures and business processes

The structure of the organisation’s logical and physical information assets, information management resources

Individual applications to be deployed, their interactions and relationships to support business outcomes

Software, hardware and network infrastructure necessary to support the application systems and databases

Plan – Technology Adoption using Gartner's "Hype Cycle"
Plan – Proposed Framework for Managing Technology Adoption

Plan – Cater for adopting technologies at different stages of maturity
What is an “ESOE”?  

- It's essentially a system that tackles some hard problems associated with electronic collaboration, to make it easier for end users to work, with some extra perks for administrators.

- It’s middleware, so if you can’t see it, then it’s doing its job.

- It’s standards based, it’s open source, it’s the latest Java technologies and software development methodologies.

- It takes care of Authentication, Single Sign On (there is a difference!) creation of authorization policies and enforcement of access control. It federates with business partners easily. Your electronic content is more accessible and more secure at the same time.

Why did we build it?

- There was a need for a new identity management and SSO system, nothing in the market place could really solve our needs and we looked around a lot for something to solve our problems.

- We want to make access to electronic resources easy for our students and staff, less to remember and easier to use at QUT and externally, otherwise you end up with....

- We’re into Shibboleth, OpenID and others, we wanted to use the technologies widely but reduce the complexity of getting them running, while at the same time being able to extend to new technologies in the future.
What is the design based on?

• **OPEN STANDARDS** of course!

• **SAML 2.0** - Security Assertion Markup Language - an XML-based framework for ensuring that transmitted communications are secure. SAML defines mechanisms to exchange authentication, authorization and nonrepudiation information, allowing single signon capabilities for Web services.

  We have SAML 2.0 libraries in Java and C++ you can use today if you’re working in the field.

• **XACML 2.0** - eXtensible Access Control Markup Language - an XML-based framework that expresses security policies and access rights to information for Web services, digital rights management (DRM), and enterprise security applications. We didn’t quite implement the full XACML 2.0 spec because some of it simply isn’t relevant, so to avoid confusion we term our implementation LXACML.
What authentication sources does ESOE support?

• The short answer is anything you like.

• The longer answer is we’ve written implementations for LDAP and Active Directory but with the plugin architecture we have defined you could write a module to authenticate from any source, even a flat file if you so desire (and yes we did it in testing).

• The pipeline can also allow you to do multiple authentications over time, increasing for example levels in multi-factor scenario which can then be used as a basis for access control.

• ESOE is able to support multiple authentication sources at the same time with its pipelined authentication design if some users have an account in one LDAP server and others in a database for example both can be used as sources of authentication at the same time.
How does ESOE do access control?

- Everything is based on LXACML policies which are very flexible and allow fine grained control over who can access what. This is very important when you consider that ESOE allows people to come into the system from basically anywhere.

- Each application deploys a piece of software called a Service Provider Enforcement Point “SPEP”. This software does a number of things to communicate with the ESOE but the most important job it does is access control. **And this is easier to do than Shibbing the app**

- For each resource request (lets say /secure/index.jsp) the SPEP will send a message to the ESOE to ask if this is allowed. The ESOE, based on all the knowledge it has about the principals identity and in combination with the LXACML policy will return a Permit or Deny statement. The SPEP then acts accordingly allowing the request to pass or denying it.

- Our SPEP software also does some interesting things with caching though the algorithm and math is complex and I won’t bore you all to death with specifics, needless to say its designed to prevent “ESOE death”. See the team.

- Additionally ESOE authorization can work hand in hand with existing access control features already in applications.
How does ESOE support Federation?

- ESOE has a centralized design, every SPEP in the authentication network is connected to it at all times.
- If ESOE has modules written to understand it then applications automatically understand it.
- Currently ESOE is able to communicate with users authenticating via: Shibboleth 1.3.x, OpenID 1.x and 2.x
- In the future we may expand to support Yahoo BBAuth, WS-Federation and others.
- We’re working with Google on some interesting code that may prove very useful in the federated application space.
What attributes have been released to QUT?

The following details have been provided to QUT. Please ensure you wish to release these details then click continue below:

You are about to release the following information as part of using services provided by this site:

<table>
<thead>
<tr>
<th>Name</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td><a href="mailto:smith@qut.edu.au">smith@qut.edu.au</a></td>
</tr>
<tr>
<td>an</td>
<td>Smith</td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:lammith@qut.edu.au">lammith@qut.edu.au</a></td>
</tr>
<tr>
<td>givenName</td>
<td>Terence</td>
</tr>
<tr>
<td>email-externalised-identity</td>
<td>True</td>
</tr>
<tr>
<td>esc-externalised-identity</td>
<td></td>
</tr>
<tr>
<td>esc-delegator</td>
<td>shibboleth</td>
</tr>
</tbody>
</table>

If you have trouble logging in, please contact the IT Helpdesk:

Phone: 07 3138 4000 | itHelpdesk@qut.edu.au | www.ithelpdesk.qut.edu.au

---

Processing Your Account

Your details have been entered into the QUT Blackboard system. They will take approximately 30 minutes to provision your account. Please return to the site after this time and you will be able to access the resources on QUT Blackboard.
<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
<th>Business Process Fusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>Rigid but simple Proprietary, Monolithic Application Suites and Modules</td>
<td>Remodels End-to-End Processes</td>
</tr>
<tr>
<td>2003</td>
<td>Flexible but complex Net Enabled, Services Wrapped Application.</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>Fusion &amp; consolidation SOA &amp; BPM enabled, Business Process Fusion</td>
<td></td>
</tr>
</tbody>
</table>
Platforms for Collaboration

The Data Commons
Data Federations
ANDS - $24M

Capability Computing
Advanced models
NCI - $26M

Research connectivity
Seamless reach
AAF+AREN - $6M

Collaboration services
Research workflows
ARCS - $20M

Development Team

• Bradley Beddoes - Lead Architect
  b.beddoes@qut.edu.au

• Andre Zitelli - Senior Programmer
  a.zitelli@qut.edu.au

• Shaun Mangelsdorf - Programmer
  s.mangelsdorf@qut.edu.au

• Terence Smith - Project Manager
  t.smith@qut.edu.au
http://www.esoeproject.org

“I think you should be more explicit here in step two.”